Protection concern in Mobile Cloud Computing- A Survey

Mrs. Yogita D. Mane [1],Prof. Kailas K. Devadkar[2],
[1]*(ME Department of Computer Engineering, Patel Institute of Technology, Andheri (W). University of Mumbai, India)*
[2]*(Department of Information Technology, Sardar Patel Institute of Technology, Andheri(W).University of Mumbai, India)*

ABSTRACT : *Always it is preferable to use on-demand infrastructure, provided by cloud computing instead of traditional. So the concept of Mobile Cloud Computing (MCC) come into focus. Mobile cloud computing is a technique or model in which mobile applications are built, powered and hosted using cloud computing technology. In Mobile Cloud computing we can store information regarding sender, data and receiver on cloud through mobile application. As we store more and more information on cloud by client, security issue will arise, so in this paper we have highlighted security issues in mobile cloud computing.*

Keywords - *Mobile cloud computing , Mobile computing, Cloud Computing , issues in Mobile Cloud Computing.*

I. INTRODUCTION

The mobile cloud computing is a combination of three main parts; they are mobile device, cloud computing and mobile internet. With the help Mobile Cloud Computing, a mobile user gets a rich application delivered over the Internet and powered by cloud-backed infrastructure. Now a day's the top most popular concern for mobile user or any business is Security and protection. Major Security and protection concern are mainly for mobile computing, social networks and cloud computing. Mobile cloud computing refers to the availability of cloud computing services in a mobile environment. It incorporates the elements of mobile networks and cloud computing, thereby providing optimal services for mobile users. In mobile cloud computing, mobile devices do not need a powerful configuration (e.g., CPUspeed and memory capacity) since all the data and complicated computing modules can be processed in the clouds [2, 4]. Mobile cloud computing centered are generally accessed via a mobile browser from a remote web server, typically without the need for installing a client application on the recipient phone. This concept is also sometimes referred to as MobiClo[3], a combination of MObile CLOud.

The main advantages of mobile cloud computing is as follows [8], Extending battery lifetime, Improving data storage capacity and processing power, Improving reliability and availability, Dynamic provisioning, Scalability, Multi-tenancy, Ease of Integration. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing apps and mobile computing to not just Smartphone users but a much broader range of mobile subscribers. Here we have enlisted possible benefits of Mobile Cloud Computing.

1. Mobile Cloud Computing will help to overcome limitations of mobile devices in particular of the processing power and data storage.
2. It also might help to extend the battery life by moving the execution of commutation-intensive application 'to the cloud'.
3. Mobile Cloud Computing can increase security level for mobile devices achieved by a centralized monitoring and maintenance of software.
4. It can also become a one-stop shopping option for users of mobile devices since Mobile Cloud Operators can simultaneously act as virtual network operators, provide e-payment services, and provide software, data storage ,etc. as a service.
5. A number of new technical functionalities might be provided by mobile clouds. In particular, provisioning of context- and location-awareness enables personalization of services is an attractive functionality.
6. Mobile Cloud Computing might open the cloud computing business that is currently almost exclusively addressing businesses to consumers (B2C) since they will significantly benefit from the above described options.

Further paper is divided in to 6 section, section II describe about related work, section III explain architecture of mobile cloud computing, section IV explain about difference between different issues of mobile cloud computing, section V explain briefly about security and protection concern in mobile cloud computing, section VI & VII describe need of mobile cloud computing and conclusion respectively.

II. RELATED WORK

A simple way to define “Mobile Cloud Computing is “A Mobile cloud computing is a structure where both the data storage and the data processing happen outside the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones to the cloud”. Aepona [5] describes Mobile Cloud Computing as a new paradigm for mobile applications where the data processing and storage are moved from the mobile device to powerful and centralized computing platforms located in clouds. These centralized applications are then accessed over the wireless connection based on a thin native client or web browser on the mobile devices. Weiwei Jia [6] Defines that, the benefits brought by Cloud Computing have been also demonstrated by the emergence of Mobile Cloud Computing, which is regarded as one of most disruptive technology for future mobile applications. Different from the general cloud computing concept, mobile cloud computing refers to an emerging infrastructure where both data storage and data processing happen outside of the mobile device from which an application is launched. Alternatively, Jacson H. Christensen [7] and L. Liu, R. Moulic, and D. Shea[9] Mobile Cloud Computing can be defined as a combination of mobile web and cloud computing which is the most popular tool for mobile users to access applications and services on the Internet.

III. MOBILE CLOUD COMPUTING ARCHITECTURE

Fig. 1 shows the general architecture of Mobile Cloud Computing. Where mobile devices are connected to the mobile networks via base stations (e.g., base transceiver station (BTS), access point, or satellite) that establish and control the connections (air links) and functional interfaces between the networks and mobile devices. Requests and information (e.g., ID and location) of Mobile users’ are transmitted to the central processors that are connected to servers providing mobile network services. Here, mobile network operators can provide services to mobile users as AAA (for authentication, authorization, and accounting) based on the home agent (HA) and subscribers’ data is stored in databases. After that, the subscribers’ requests are delivered to a cloud through the Internet. In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services.

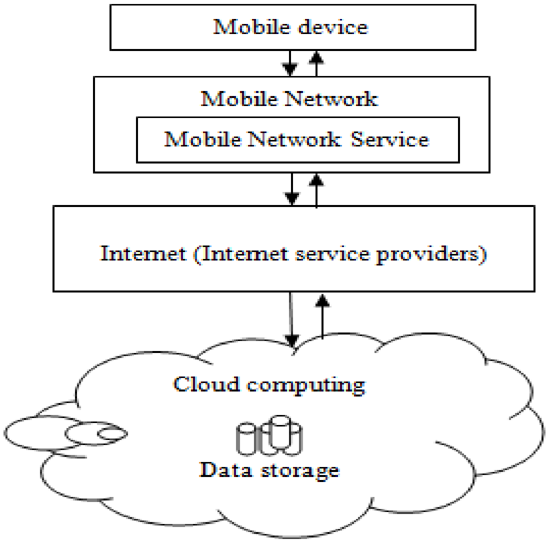

Fig.1 Architecture of MCC

IV. ISSUES IN MOBILE CLOUD COMPUTING

Issues in mobile cloud computing is broadly classify into 6 main category.

As shown in fig.2 issues are as follows- operational issues, end user issues, service level issues, privacy and security issues, context awareness and data management. Study of all issues of mobile cloud computing are given in table 1.

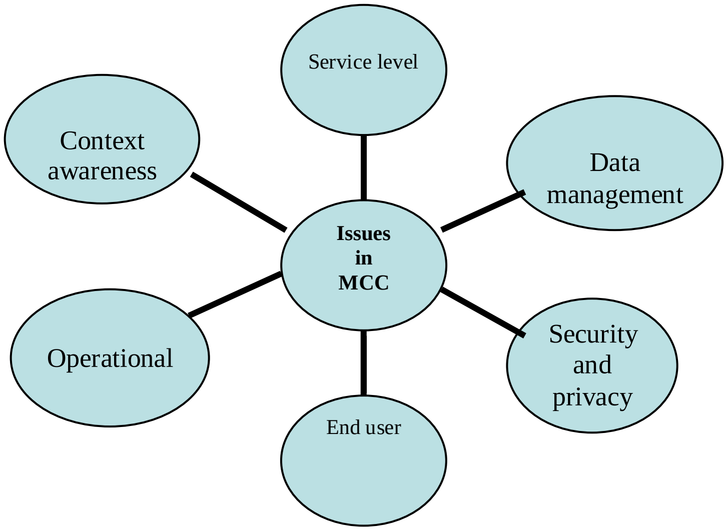

Fig. 2. Security issues in Mobile Cloud Computing.

Table 1. Difference between different issues of mobile cloud computing.

Sr. No	Type of Issues in mobile cloud computing	Methods under issue	Description about issue	Issues arise in particular type
1	Operational issue	Offloading method	Offloading job from mobile device to the cloud.	1. Physical distance from mobile device to the cloud. 2. Heterogeneity of the system being used.
		Cost benefit analysis	It determine resource usage e.g. energy and power consumption.	1. Mobility management 2. Connection protocol
2	End user issue	-	It describe regarding end user such as participating, interoperability and cost.	1. Incentives to collaborate 2. Presentation and usability issues.
3	Service and application level issue	-	This type of issue is mainly concern with performance measurement of system and QOS.	1. Availability 2. Fault tolerance
4	Privacy, security and trust	1. General cloud security 2. Mobile cloud security 3. Privacy	It mainly deals with problem of computation or data storage using cloud for mobile device	1. Low bandwidth 2. Availability 3. Heterogeneity 4. Low capacity
5	Context awareness issue	-	Provide information regarding user location, other users in surrounding area and resource in user's environment. Also use to provide information regarding resource availability and processing.	1.Context awareness mobile application may not always behave in same way the user want due to -imperfect context information -incorrect user preferences -incorrect adaption rule
6	Data management	-	Data can be access, stored and shared with external user or device	1.Data access 2. Data portability 3. Interoperability

V. MOBILE CLOUD COMPUTING SECURITY AND PRIVACY CLASSIFICATION.

Mobile devices are exposed to numerous security threats like malicious codes and their vulnerability. GPS can cause privacy issues for subscribers. Security of mobile cloud computing is divided into two main parts security modules and privacy modules. Security module mainly concern with security of mobile network and security for cloud. Security module secure the device by using authentication, access control and malware detection, whereas privacy module determines user data encryption/decryption and sensitive data management model, as shown in fig.3. Now we will see the concept of general cloud security, mobile cloud security and privacy in detail.

A) Security in Mobile Cloud Computing

Security for mobile application, one way to protect the device from installing the threat by running security software .Mobile devices are resource constrained, protecting them from the threats is more difficult than that for resourceful devices. Oberheide et al.[9] present an approach to move the threat detection capabilities to clouds. It is an extension of the CloudAV platform consisting of host agent and network service components. Host agent runs on mobile devices to inspect the file activity on a system. If an identified file is not available in a cache of previous analyzed files, this file will be sent to the include network service for verification. The second major component of CloudAV is a network service that is responsible for file verification. Portokalidis et al.[10] present a paradigm in which attack detection for a smartphone is performed on a remote server in the cloud. The smartphone records only a minimal execution trace, and transmits it to the security server in the cloud.

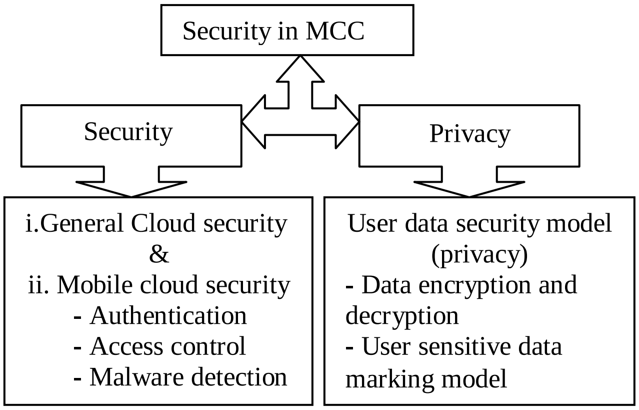

Fig. 3. Mobile Cloud Computing security and privacy classification.

B) General cloud security:

J. Brodkin, Gartner[19] summarize seven security risks that users need to consider in mobile Cloud computing;

1. Privileged user access: uploading sensitive data to the cloud would raise the problem of loss of direct physical, logical and personnel control over the data.
2. Regulatory compliance: the cloud service providers should be willing to undergo external audits and security certifications.
3. Data location: the exact physical location of user's data is not transparent, which may lead to confusion on specific authorities and commitments on local privacy requirements.
4. Data segregation: since cloud data is usually stored in a shared space, it is important each user's data is separated from others with efficient encryption schemes.
5. Recovery: it is imperative that cloud providers provide proper recovery mechanisms for data and services in case of technological failure or other disaster.
6. Investigative support: since logging and data for multiple customers may be co-located, inappropriate or illegal activity should they occur may be very hard to investigate.
7. Long-term viability: assurance that users data would be safe and accessible even if the cloud company itself goes out of business.

C) Mobile cloud security:

The simplest ways to detect security threats will be installing and running security software and antivirus programs on mobile devices. But since mobile devices are constrained with processing and power limitations, protecting them from these threats could be more difficult compared to regular computers. Several approaches have been developed transferring threat detection and security mechanisms to the cloud. Before mobile users could use a certain application, it should go through some level of threat evaluation. All file activities to be sent to mobile devices will be verified if it is malicious or not. Instead of running anti-virus software or threat detection programs locally, mobile devices only performs lightweight activities such as execution traces transmitted to cloud security servers. Security in mobile cloud computing, between mobile device and user is determine by three main parts authentication, access control and malware detection. To make the secure communication between mobile device and cloud, X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, S. Jeong,[20] propose the Securing elastic applications on mobile devices for cloud computing, name as 'weblet'.' Weblet' is use to migrate the data/information to and from mobile device and cloud. So as far as security concern, it include 3 main parts, they are explain as follows.

1. Authentication between the 'weblets' that would be distributed between the cloud and the device,
2. Authorization for weblets that could be executing on relatively untrusted cloud environments to access sensitive user data.
3. Establishment and verification of trusted 'weblet' execution of cloud nodes.

The secure elastic application framework for weblet is based on the assumption that the cloud elasticity service (CES), including the cloud manager, application manager, cloud node manager, and cloud fabric interfaces (CFI), is honest. The security threats are categorized as threats to mobile devices, threats to cloud platform and application container, and threats to communication channels. So that the authors propose a framework with the following security objectives: Trustworthy weblet containers (VMs) on both device and cloud, authentication and secure session management needed for secure communication between weblets and multiple instantiation concurrently, authorization and access control enforcing weblets on the cloud to have the lowest privileges, and logging and auditing of weblets.

Privacy Issues in Mobile Cloud Computing: In [21], M. Fahrmair, W. Sitou, B. Spanfelner, Security and privacy rights management for mobile and ubiquitous computing, presents the following requirements of a mobile and ubiquitous system that satisfies user privacy for both mobile device and cloud, they are as follows protection against misuse, identification of pirated datasets, adjustment of laws (to provide additional security under certain circumstances), and ease of use.

Location based services (LBS) faces a privacy issue on mobile users' provide private information such as their current location. This problem becomes even worse if an opponent knows user's important information. Zhangwei and Mingjun [11] propose the location trusted server (**LTS**) approach. After receiving mobile users' requests, LTS gathers their location information and cloaks the information called "cloaked region" to conceal user's information. The "cloaked region" is sent to LBS, so LBS knows only general information about the users but cannot identify them.

Digital Rights Management(DRM): DRM is used to protect digital contents from illegal access. Phosphor is a cloud based mobile digital rights management (DRM) scheme with improved flexibility and reduced vulnerability at a low cost. A License State Word (LSW) located in a sim card and the LSW protocol based on the application protocol data unit (APDU, the smart card comm. std) command are provided. When a mobile user receives the encrypted data, he/she uses the decryption key from a sim card via APDU command to decode.

VI. NEED OF PROTECTION AND ISSUES IN PROTECTION

So with the help of above discussion we conclude that, a major issue with the mobile cloud is the resource limitation for mobile devices, such as small screen size, less memory capacity, limited battery power as compared with desktop computers. Because of the resource limitation, the mobile cloud is most often viewed as an *SaaS cloud*, which mean that computation and data handling are usually performed in the cloud. e.g. Smart phones which is often use web browser to access the cloud.

other reasons which affect the mobile cloud is Latency and bandwidth. To improve the latency we can use Wi-Fi but it may decrease bandwidth when many mobile devices are present. There are some reason which affect the Bandwidth for 3G cellular is limited by cell tower bandwidth in some areas. Similarly, connectivity may be intermittent. As cellular providers build out their networks, the situation will improve, but dead spots won't completely disappear.

With above discussion we notice that application security has become a primary protection concern for mobile users, as mobile devices usually carries highly sensitive personal information. Compared to traditional desktop, if we are downloading some application from cloud, we can able to provide security in terms of, malware and virus detection, and information leak detection. These can possible by just installing antivirus for the desktop, but this is not possible for mobile device because of above mention issues such as limited battery, small screen size, less memory capacity. To overcome this problem [23] COSMOS that is **C**loud **O**rchestrated **S**ervices for **MO**bile **S**ecurity, this infrastructure is use to support heterogeneous devices in terms of both architectures and platforms, and will leverage virtualization to provide services for securing mobile applications. In this context, the cloud computing paradigm can be force to offload security-oriented functions from the devices to the cloud infrastructure. Furthermore, mobile applications can be encapsulated in a virtual environment in the cloud, and transparently accessed by mobile users through a remote connection.

VII. CONCLUSION

Mobile cloud computing is consisting of 3 main parts with their main advantages they are mobile device, mobile internet and cloud computing, hence mobile cloud computing use to provide bet possible services for mobile users.

Mobile Cloud Computing integrates the cloud computing into the mobile environment so that it is use to overcomes disadvantage related to the performance such as battery life, storage, and bandwidth, environment such as heterogeneity, scalability, and availability, and security such as reliability and privacy discussed in mobile computing.

This paper we have discussed regarding protection concern in Mobile Cloud Computing, which is consisting of introduction , all issues but briefly security issues of mobile cloud computing. Securing mobile cloud computing user's privacy and integrity of data or applications is one of the key issues most cloud providers are given attention. Since mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into two categories: mobile network user's security; and mobile cloud security.

REFERENCES

[1]http://andromida.hubpages.com/hub/cloud-computing-architecture.

[2] http://www.mobilecloudcomputingforum.com/

[3] MobiCloud: Building Secure Cloud Framework for Mobile Computing And Communication, 2010 Fifth IEEE International Symposium on Service Oriented System Engineering.

[4]http://www.readwriteweb.com/archives/why_cloud_computing_is_the_future_of_mobile.php.

[5] White Paper, "Mobile Cloud Computing Solution Brief," AEPONA, November 2010.

[6] SDSM: A Secure Data Service Mechanism in Mobile Cloud Computing 978-1-4577-0248-8/11/$26.00 ©2011 IEEE

[7] Jacson H. Christensen, "Using RESTful web-services and cloud computing to create next generation mobile applications," in Proceedings of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications (OOPSLA), pp. 627-634, October 2009.

[8] A Survey of Mobile Cloud Computing:Architecture, Applications, and Approaches by Hoang T. Dinh, Chonho Lee, Dusit Niyato.

[9] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian. "Virtualized in-cloud security services for mobile devices," in Proc 1st Workshop on Virtualization in Mobile Computing (MobiVirt), pp. 31-35, June 2008.

[10] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid Android: versatile protection for smartphones," in Proc 26th Annual Computer Security Application Conference (ACSAC), pp. 347-356, September 2010.

[11] H. Zhangwei and X. Mingjun, "A Distributed Spatial Cloaking Protocol for Location Privacy," in Proc 2nd Intl Conf on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2, pp. 468, June 2010.

[12] W. Itani, A. Kayssi, and A. Chehab, "Energy-efficient incremental integrity for securing storage in mobile cloud computing," International Conference on Energy Aware Computing (ICEAC), pp. 1, January 2011.

[13] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, "Authentication in the clouds: a framework and its application to mobile users," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW), pp. 1-6, 2010.

[14] Mobile cloud computing: A survey Niroshinie Fernando , Seng W. Loke , Wenny Rahayu Department of Computer Science and Computer Engineering, La Trobe University, Australia

[15] E. Walker, W. Brisken, J. Romney, To lease or not to lease from storage clouds, Computer 43 (2010) 44–50

[16] X. Jin and Y. K. Kwok, "Cloud Assisted P2P Media Streaming for Bandwidth Constrained Mobile Subscribers," in Proceedings of the 16th IEEE International Conference on Parallel and Distributed Systems (ICPADS), pp. 800, January 2011.

[17] G. Huerta-Canepa and D. Lee, "A virtual cloud computing provider for mobile devices," in Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond (MCS), no. 6, 2010

[18] A. Klein, C. Mannweiler, J. Schneider, and D. Hans, "Access Schemes for Mobile Cloud Computing," in Proceedings of the 11th international Conference onMobile Data Management (MDM), pp. 387, June 2010

[19] J. Brodkin, Gartner: Seven cloud-computing security risks. http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853, 2008.

[20] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, S. Jeong, Securing elastic applications on mobile devices for cloud computing, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, CCSW'09, ACM, New York, NY, USA, 2009, pp. 127–134.

[22] M. Fahrmair, W. Sitou, B. Spanfelner, Security and privacy rights management for mobile and ubiquitous computing, in: Workshop on UbiComp Privacy, pp. 97–08

[23]http://crewman.uta.edu/projects/cloud-orchestrated-services-for-mobile-security